What is claimed is:

1. A system for providing dynamic screening of transient messages in a distributed computing environment, comprising:

an antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a header comprising a plurality of address fields storing contents;

a stored set of blocking rules, each blocking rule defining readily-discoverable characteristics indicative of messages infected with at least one of a computer virus, malware and bad content;

a parser module identifying the contents of each address field;

a comparison module checking the contents of each address field against the blocking rules to screen infected messages and identify clean messages; and

an intermediate message queue staging each such clean message pending further processing.

2. A system according to Claim 1, further comprising:

a message receiver discarding each such infected message without further processing.

3. A system according to Claim 1, wherein each such blocking rule is specified as a regular expression containing at least one of literal and wildcard values.

4. A system according to Claim 1, further comprising:

an antivirus scanner scanning each message in the intermediate message queue for at least one of a computer virus, malware and bad content.

5. A system according to Claim 4, further comprising:

an event handler performing each scanning operation as an event responsive to each such clean message staged in the intermediate message queue.

6. A system according to Claim 1, further comprising:

a gateway receiving the incoming messages into the network domain boundary.

7. A system according to Claim 1, wherein the structured fields comprise at least one of sender, recipient, copied recipient, blind copied recipient, date, time, and subject.

8. A system according to Claim 1, wherein the incoming message comprises at least one attachment.

9. A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

10. A method for providing dynamic screening of transient messages in a distributed computing environment, comprising:

intercepting an incoming message at a network domain boundary, the incoming message including a header comprising a plurality of address fields storing contents;

maintaining a set of blocking rules, each blocking rule defining readily-discoverable characteristics indicative of messages infected with at least one of a computer virus, malware and bad content;

identifying and checking the contents of each address field against the blocking rules to screen infected messages and identify clean messages; and

staging each such clean message into an intermediate message queue pending further processing.

11. A method according to Claim 10, further comprising:

discarding each such infected message without further processing.

12. A method according to Claim 10, further comprising:

specifying each such blocking rule as a regular expression containing at least one of literal and wildcard values.

13. A method according to Claim 10, further comprising:

scanning each message in the intermediate message queue for at least one of a computer virus, malware and bad content.

14. A method according to Claim 13, further comprising:

performing each scanning operation as an event responsive to each such clean message staged in the intermediate message queue.

15. A method according to Claim 10, further comprising:

receiving the incoming messages at a gateway into the network domain boundary.

16. A method according to Claim 10, wherein the structured fields comprise at least one of sender, recipient, copied recipient, blind copied recipient, date, time, and subject.

17. A method according to Claim 10, wherein the incoming message comprises at least one attachment.

18. A method according to Claim 10, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

19. A computer-readable storage medium holding code for performing the method according to Claims 10, 11, 12, 13, 14, 15, 16, 17, or 18.

20. A system for efficiently detecting computer viruses and malware at a network domain boundary, comprising:

an antivirus system receiving an incoming message packet from a sending client at a network domain boundary through an open connection, the incoming message packet comprising a header including fields, which each store field values;

a message receiver comprising:

a parser module parsing the field values from each field in the header of each incoming message packet by extracting tokens representing the field values;

a comparison module comparing the tokens to characteristics indicative of at least one of a computer virus and malware to identify screened incoming message packets, and forwarding each screened incoming message packet.

21. A system according to Claim 20, wherein each incoming message packet further comprises a body storing message content, further comprising:

an antivirus scanner scanning the message content of the body of each screened incoming message packet for at least one of a computer virus and malware to identify uninfected screened incoming message packets, and forwarding each uninfected screened incoming message packet.

22. A system according to Claim 20, further comprising:

a message queue enqueueing each screened incoming message packet.

23. A system according to Claim 20, wherein the antivirus system closes the open connection to the sending client of each non-screened incoming message packet.

24. A system according to Claim 20, wherein the comparison module analyzes at least one of a sender, recipient, copied recipient, blind copied recipient, date, time, and subject field in the header of each incoming message packet.

25. A system according to Claim 20, wherein the comparison module applies blocking rules to the field values of the header of each incoming message packet.

26. A system according to Claim 20, wherein the distributed computing environment is TCP/IP-compliant and each incoming message packet is SMTP-compliant.

27. A method for efficiently detecting computer viruses and malware at a network domain boundary, comprising:

receiving an incoming message packet from a sending client at a network domain boundary through an open connection, the incoming message packet comprising a header including fields, which each store field values;

parsing the field values from each field in the header of each incoming message packet by extracting tokens representing the field values;

comparing the tokens to characteristics indicative of at least one of a computer virus and malware to identify screened incoming message packets; and

forwarding each screened incoming message packet.

28. A method according to Claim 27, wherein each incoming message packet further comprises a body storing message content, further comprising:

scanning the message content of the body of each screened incoming message packet for at least one of a computer virus and malware to identify uninfected screened incoming message packets; and

forwarding each uninfected screened incoming message packet.

29. A method according to Claim 27, further comprising:

enqueueing each screened incoming message packet onto a message queue.

30. A method according to Claim 27, further comprising:

closing the open connection to the sending client of each non-screened incoming message packet.

31. A method according to Claim 27, further comprising:

analyzing at least one of a sender, recipient, copied recipient, blind copied recipient, date, time, and subject field in the header of each incoming message packet.

32. A method according to Claim 27, further comprising:

applying blocking rules to the field values of the header of each incoming message packet.

33. A method according to Claim 27, wherein the distributed computing environment is TCP/IP-compliant and each incoming message packet is SMTP-compliant.

34. A computer-readable storage medium holding code for performing the method according to Claims 27; 28, 29, 30, 31, 32, or 33: